IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA
MINNEAPOLIS DIVISION

Muhammad Zahid, individually and on behalf all others similarly situated,

Plaintiff(s),

v.

Fortra LLC,

Defendant.

CASE NO._____

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Muhammed Zahid ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Fortra LLC ("Defendant"), a Minnesota corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach in January 2023 ("Data Breach") on Defendant's network that resulted in unauthorized access to customer and employee data.

2. Plaintiff and Class Members provided their PII to Hatch Back who, upon information and belief, contracted with Defendant to store and protect Plaintiff's and Class Members' PII.

3. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant and its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

4. Information compromised in the Data Breach includes Defendant's customers' and (current and former) employees' name and Social Security number (collectively, "PII").

5. As a result of the Data Breach, Plaintiff and approximately 139,493 Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, invasion of privacy, and the valuable time spent that was reasonably incurred to remedy or mitigate the effects of the attack.

6. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained.

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml (last visited: March 6, 2023).

7. As explained below, Defendant's inadequate cybersecurity measures enabled an unauthorized third party to gain access to Defendant's network and obtain Plaintiff's and Class Members' PII, including name and Social Security Number.

8. On or around February 28, 2023, Plaintiff received a Notice of Security Incident Letter ("Notice of Data Breach"), which informed him that:

> **What Happened?** On January 29, 2023, [Defendant] experienced a cyber incident when they learned of a vulnerability located in their software. On February 3, 2023, Hatch Bank was notified by [Defendant] of the incident and learned its files contained on [Defendant's] GoAnywhere site were subject to unauthorized access. [Defendant's] investigation determined that, between January 30 and January 31, 2023, someone without authorization had access to certain files stored within [Defendant'] GoAnywhere site. [Defendant] launched a diligent and comprehensive review of relevant files to determine the information that may have been impacted.
>
> **What Information was Involved?** On February 7, 2023, [Defendant] determined the information may have been impacted by this incident includes [Plaintiff's] name and Social Security number. Again, at this time [Defendant] has no indication that your information was subject to an actual or attempted misuse as a result of this incident.[2]

9. Defendant maintained the PII in a reckless and negligent manner.

10. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks.

11. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known

[2] *Id.*

risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

12. Through its Notice of Data Breach, Defendant admits that the Data Breach was caused, at least in part, due to "vulnerability[ies] located in [its] software."

13. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves.

14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.,* opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims on behalf of the Class (defined *infra*) for negligence and negligence *per se*.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are

more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[3]

21. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the many of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

22. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

PARTIES

23. Plaintiff Muhammed Zahid is, and at all times mentioned herein was, an individual citizen of the State of Florida. Plaintiff received a data breach notice letter dated February 28, 2023, informing him that his PII, including his name and Social Security Number, was compromised in the Data Breach.

24. Defendant Fortra LLC is a limited liability company organized and registered according to the laws of the State of Delaware. Defendant maintains its primary headquarters in Eden Prairie, Minnesota. Defendant's principal place of business is located at 11095 Viking Drive, Suite 100, Eden Prairie, Minnesota, 55344.

[3] According to the report submitted to the Maine Attorney General office, 631 Maine residents were impacted. *See id.*

DEFENDANT'S BUSINESS

25. Defendant provides information technology management software and services. The Company offers automation, cybersecurity, monitoring solutions, product training, implementation, configuration, upgrades, conversion services. Help/Systems serves customers worldwide.[4]

26. On its website, Defendant refers to itself as "Your Cybersecurity Ally" and offers services such as vulnerability management, offensive security, email security & Anti-Phishing, Data Protection, Digital Risk Protection, and Secure File Transfer.[5]

27. On information and belief, in the ordinary course of business, Defendant contracts with companies to store and protect client information, including names and Social Security numbers.

28. On information and belief, Plaintiff and Class Members provided their PII to Hatch Bank who, in turn, hired Defendant to store and protect Plaintiff's and Class Members' PII.

29. By accepting Plaintiff's and Class Members' PII, Defendant promised to provide confidentiality and adequate security for this PII.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff

[4] https://www.bloomberg.com/profile/company/6721124Z:US?leadSource=uverify%20wall (last visited: March 6, 2023).
[5] https://www.fortra.com/ (last visited: March 6, 2023).

and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PII from unauthorized disclosure.

31. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

32. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

33. Defendant experienced a Data Breach on or around January 29, 2023.

34. On February 3, 2023, Defendant notified Hatch Bank that its systems had been subject to the Data Breach. Specifically, Defendant stated that an actor had gained unauthorized access to Defendant's network.

35. On February 7, 2023, Defendant determined that information on its systems may have included names and Social Security numbers.

36. On information and belief, the investigation revealed that approximately 139,493 individuals were victims of the Data Breach.[6]

37. Plaintiff and Class Members provided their PII to Defendant with the

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml (last visited: March 6, 2023).

reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

38. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

39. In light of recent high-profile data breaches at other companies similar to Defendant, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

40. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

41. In fact, according to the cybersecurity firm PurpleSec, a survey of 1,100 IT professionals showed 90% of clients had suffered a ransomware attack in the past

[7]*FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 23, 2021).

year.[8]

42. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

50. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to

[8] *2021 Cyber Security Statistics, The Ultimate List of Stats, Data, & Trends*, https://purplesec.us/resources/cyber-securitystatistics/#:~:text=Of%20the%201%2C100%20IT%20professionals,every%2011%20seconds%20by%202021 (last visited Mar. 15, 2022).

[9] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 24, 2021).

expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. Defendant failed to properly implement basic data security practices.

55. Defendant's failure to employ reasonable and appropriate measures to protect against and detect unauthorized access to customers' PII constitutes an unfair

[10] *Id.*

act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Defendant was at all times fully aware of its obligation to protect the PII of their customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

57. As shown above, several best practices have been identified that a minimum should be implemented by IT services companies, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

58. Other best cybersecurity practices that are standard in the IT services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

59. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,

PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

60. These foregoing frameworks are existing and applicable industry standards in the IT services industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

DEFENDANT'S BREACH

61. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

i. Failing to adhere to industry standards for cybersecurity.

62. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' PII by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted PII.

63. Accordingly, as outlined below, Plaintiff and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft

64. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

65. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[11]

66. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[12]

67. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[13]

68. That is because any victim of a data breach is exposed to serious

---

[11] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Aug. 24, 2021).

[12] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Aug. 25, 2021).

[13] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 25, 2021).

ramifications regardless of the nature of the data.

69. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names.

70. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

71. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

72. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

73. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit

reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[14]

74. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

75. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

76. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

77. Moreover, theft of PII is also gravely serious. PII is an extremely valuable property right.[15]

78. Its value is axiomatic, considering the value of "big data" in corporate

[14] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited Aug. 25, 2021).

[15] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

79. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

80. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

81. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

82. There is a strong probability that entire batches of information stolen from Defendant have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a present and substantially increased risk of fraud and identity theft for many years into the future.

83. Thus, Plaintiff and Class Members must vigilantly monitor their

financial and medical accounts for many years to come.

84. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[16]

85. PII particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

86. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[17] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[18]

87. Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an

[16] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Aug. 25, 2021).
[17] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 25, 2021).
[18] *Id* at 4.

individual's authentic tax return is rejected.

88. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

89. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[20]

90. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

---

[19] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 25, 2021).

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 25, 2021).

Plaintiff Zahid's Experience

85. Plaintiff Muhammed Zahid indirectly provided his PII to Hatch Bank who, on information and belief, contracted with Defendant to store Plaintiff's and Class Members' PII.

86. On or about February 28, 2023, Plaintiff received a Notice of Data Breach from Defendant informing him that his PII had been impacted by the Data Breach, including his name and Social Security number.

87. As a result of the Data Breach, Defendant directed Plaintiff to take certain steps to protect his PII and otherwise mitigate his damages.

88. As a result of the Data Breach and the information that he received in the Notice Letter, Plaintiff has spent significant time dealing with the consequences of the Data Breach, including contacting each of the three major credit bureaus to place credit freezes on his accounts. Valuable time that has been lost forever and cannot be recaptured.

89. Plaintiff is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

90. Plaintiff stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his

identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

91. Plaintiff suffered actual injury and damages due to Defendant's mismanagement of his PII before the Data Breach.

92. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII —a form of intangible property that he entrusted to Defendant, which was compromised in and as a result of the Data Breach.

93. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy since he received the Notice of Data Breach Letter. Plaintiff is especially concerned about the theft of his full name paired with his Social Security number.

94. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

95. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Common Injuries and Damages

103. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

104. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

105. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

106. Plaintiff's PII was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's computer system.

107. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

108. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

109. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

110. Plaintiff and Class Members face the present and substantially increased risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

111. Plaintiff and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

112. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

113. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

114. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer network and Plaintiff

and Class Members' PII. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

115. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

116. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected

from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

117. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

CLASS ACTION ALLEGATIONS

118. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

119. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a Notice of Data Breach (the "Class").

120. The proposed Class is referred to collectively as the "Class." Members of the Class are referred to collectively as "Class Members."

121. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal

representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

122. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

123. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 140,000 individuals whose PII was compromised in the Data Breach.[21]

124. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

[21] https://apps.web.maine.gov/online/aeviewer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml (last accessed Mar. 13, 2023).

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached a fiduciary duty to Plaintiff and Class Members;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, treble damages, and/or injunctive relief.

125. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

126. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions.

127. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

128. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have

no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

129. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

124. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 123 above as if fully set forth herein.

125. Defendant required Plaintiff and Class Members to submit non-public personal information as a condition of employment (or prospective employment) and/or as a condition of purchasing goods and services from Defendant.

126. By collecting and storing this data in its computer property, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the

information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

128. Defendant's duty of care to use reasonable security measures arose because Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from the Data Breach.

129. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security

measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised;

f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

131. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the past few years.

132. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

133. Plaintiff and Class Members are entitled to compensatory and

consequential damages suffered as a result of the Cyber-Attack and data breach.

134. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

135. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 134 above as if fully set forth herein.

136. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

137. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

138. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

139. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

140. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

141. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

142. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their PII.

143. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: March 13, 2023

Respectfully Submitted,

/s/David A. Goodwin
Daniel E. Gustafson (MN Lic. #202241)
David A. Goodwin (MN Lic. #0386715)
Joe E. Nelson (MN Lic. #0402378)
GUSTAFSON GLUEK PLLC
120 South Sixth Street, Suite 2600
Minneapolis, MN 55402
Tel: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
Jnelson@gustafsongluek.com

Joseph M. Lyon*
THE LYON LAW FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

**pro hac vice forthcoming*

Attorneys for Plaintiff and the Proposed Class